UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/759,409	01/16/2004	Luciano M. Silva	RSW920030258US1 (140)	7485

46320 7590 11/05/2008
CAREY, RODRIGUEZ, GREENBERG & PAUL, LLP
STEVEN M. GREENBERG
950 PENINSULA CORPORATE CIRCLE
SUITE 3020
BOCA RATON, FL 33487

EXAMINER	
PARK, JEONG S	
ART UNIT	PAPER NUMBER
2454	
MAIL DATE	DELIVERY MODE
11/05/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 10/765,304
Filing Date: January 27, 2004
Appellant(s): FORD ET AL.

Luciano M. Silva
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 7/21/2008 appealing from the Office action mailed 2/20/2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2003/0167298	Bazinet et al.	09-2003
6,985,946	Vasandani et al.	01-2006
2006/0004887	Schenk, Andre	01-2006

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 4 and 6-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bazinet et al. (hereinafter Bazinet)(U.S. Pub. No. 2003/0167298 A1), and further in view of Vasandani et al. (hereinafter Vasandani)(U.S. Patent No. 6,985,946 B1).

Regarding claim 4, Bazinet teaches as follows:

a system for programmatic role-based security in a dynamically generated user interface, the system comprising:

an application framework configured through a deployment descriptor (portal generic objects database) comprising a listing of a set of views (n generic objects 204 in figure 2, each object creates different view), a listing of associated program logic (based on the access privileges of the authenticated user the database lists different access level) and a listing of a set of authorized actions (read, read/write, or no access, 208 in figure 2, indicates the roles) for selected ones of said views (see, e.g., page 2, paragraph [0030]);

a first view (502 in figure 5) listed in said deployment descriptor (portal generic objects database) and comprising a linkage to a second view (linkage to the backend applications 126 in figure 1) listed in said deployment descriptor (the portal application generates a page to the client containing entries corresponding to the backend applications that the authenticated user can access based on the access privileges of the authenticated user, see, e.g., page 3, paragraphs [0038] and figure 5); and

access checking logic disposed in said first view and programmed to omit said linkage (no access) where a role of an end user accessing said first view is not authorized to access said second view according to said listing of said set of authorized roles in said deployment descriptor (the instructions, 506 in figure 5, only shows what are authorized to the client, see, e.g., page 4, paragraph [0040] and figure 5).

Bazinet does not teach the security control by user roles.

Vasandani teaches as follows:

providing role based access security within a networked computing system (see, e.g., col. 2, lines 40-43); and

the method for providing an authentication and authorization pipeline having a userID-roles database and a resource-roles database for use in a web server to grant access to web resources to users (see, e.g., col. 2, line 58 to col. 3, line 9).

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Bazinet to include the method of role based security access as taught by Vasandani in order to efficiently control security access by the user's roles predefined.

Regarding claim 6, Bazinet teaches as follows:

said program logic comprises servlets and wherein said views comprise Java server pages (the Web page sent by the portal server to the clients may include Java server pages, see, e.g., page 2, paragraph [0026], lines 12-17).

Regarding claim 7, Bazinet teaches as follows:

a custom tag (instructions 506 in figure 5, see, e.g., page 4, paragraph [0039]) disposed in said first view for invoking said access checking logic and for omitting said linkage responsive to said access checking logic (the first Web page shows the instruction tag for users to select eligible applications based on the access privileges of the authenticated user, see, e.g., page 3, paragraph [0030] and [0038]).

Regarding claim 8 and 12, Bazinet teaches as follows:

a method for programmatic user privilege based security in a dynamically generated user interface (see, e.g., abstract), the method comprising the steps of:

authenticating access to a rendering of a selected view based upon an end user's privileges (access privileges of the authenticated user) requesting access to said selected view (see, e.g., step 414 in figure 4 and page 3, paragraph [0037]);

processing said selected view to identify a method call to access checking logic (see, e.g., steps 422-434 in figure 4 and page 4, paragraphs [0042]-[0044]); and

disposing a link to said different view in said rendering of said selected view conditional upon said role matches a role in said set of roles (the privilege stored in the portal generic objects database)(the portal application generate a page to the client containing entries corresponding to the backend applications that the authenticated user can access based on the access privileges of the authenticated user, see, e.g., page 3, paragraph [0038] and step 416 in figure 4).

Bazinet does not teach role based security access and following steps of using it but all limitations with user's privilege based security access.

Vasandani teaches as follows:

providing role based access security within a networked computing system (see, e.g., col. 2, lines 40-43);

the method for providing an authentication and authorization pipeline having a userID-roles database and a resource-roles database for use in a web server to grant access to web resources to users (see, e.g., col. 2, line 58 to col. 3, line 9); and

comparing said role (userID-roles object, 211 in figure 4) to a set of roles (roles/access database, 422 in figure 4) authorized to access a different view (requested resource) associated with said access checking logic (the roles authorization module retrieves the database entry for the requested resource using the URI and attempts to match a role from the userID-roles object with the roles in the roles/access database entry, see, e.g., col. 8, lines 1-4).

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Bazinet to include the method of role based security access as taught by Vasandani in order to efficiently control security access by the user's roles predefined.

Regarding claims 9-11 and 13-15, Vasandani teaches as follows:

said step of authenticating comprises the step of comparing said role (userID-roles object, 211 in figure 4) to a set of roles (roles/access database, 422 in figure 4) associated with said selected view to locate a match for said role (the roles authorization module retrieves the database entry for the requested resource using the URI and attempts to match a role from the userID-roles object with the roles in the roles/access database entry, see, e.g., col. 8, lines 1-4);

said locating step comprises the step of parsing a deployment descriptor (roles/access database, 422 in figure 4) for an application framework hosting said selected view and said different view to identify said set of roles (this is inherent process for authorization module 202 in figure 4, see, e.g., col. 7, line 53 to col. 8, line 11); and

said processing step comprises the step of invoking external access checking logic for a located server page tag referencing said access checking logic (this is inherent process for authorization module 202 in figure 4, see, e.g., col. 7, line 53 to col.

8, line 11).

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Bazinet to include the method of role based security access as taught by Vasandani in order to efficiently control security access by the user's roles predefined.

Regarding claim 16, Bazinet teaches as follows:

A method for programmatic user privilege based security in a dynamically generated user interface (see, e.g., abstract), the method comprising the steps of:

configuring a deployment descriptor (portal generic objects database, 203 in figure 2)(populating a portal generic object database, see, e.g., page 3, paragraph [0032]); and

composing a server page to include a reference to said external access checking logic and to invoke said external access in order to conditionally incorporate a link to a specific view associated with a specific set of authorized roles (the portal application, 102 in figure 1 and 502 in figure 5, generates a page to the client containing entries corresponding to the backend applications, see, e.g., page 3, paragraph [0038]).

Vasandani teaches as follows:

providing role based access security within a networked computing system (see, e.g., col. 2, lines 40-43);

the method for providing an authentication and authorization pipeline having a userID-roles database and a resource-roles database for use in a web server to grant access to web resources to users (see, e.g., col. 2, line 58 to col. 3, line 9); and programming external access checking logic to match a parameterized role (userID-roles object, 211 in figure 4) with a role disposed in said set of roles in said deployment descriptor (roles/access database, 422 in figure 4)(the roles authorization module retrieves the database entry for the requested resource using the URI and attempts to match a role from the userID-roles object with the roles in the roles/access database entry, see, e.g., col. 8, lines 1-4).

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Bazinet to include the method of role based security access as taught by Vasandani in order to efficiently control security access by the user's roles predefined.

Regarding claim 17, Bazinet teaches as follows:

said access checking logic is programmed to display said linkage where a role of the end user accessing said first view is authorized to access said second view (the portal application generate a page (equivalent to applicant's said linkage) to the client containing entries corresponding to the backend applications that the authenticated user can access based on the access privileges of the authenticated user, see, e.g., page 3, paragraphs [0038] and [0039]).

Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bazinet et al. (hereinafter Bazinet)(U.S. Pub. No. 2003/0167298 A1) and Vasandani et al. (hereinafter Vasandani)(U.S. Patent No. 6,985,946 B1) as applied to claim 4 above, and further in view of Schenk (U.S. Pub. No. 2006/0004887 A1).

Regarding claim 5, Bazinet and Vasandani teach all the limitations of claim 4 as explained above except for using Struts framework as the application framework incorporating the JSPs.

Schenk teaches as follows:

a configuration file is used to configure the presentation of an object (see, e.g., page 2, paragraph [0015]); and

Java server pages can be generated with Struts framework, as open source framework of utilizing pre-stored design patterns (see, e.g., page 2, paragraph [0017], lines 15-19).

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Bazinet and Vasandani to include Struts framework as an application framework incorporating the JSPs as taught by Schenk in order to facilitate the development of JSPs applications.

(10) Response to Argument

A. Appellants' arguments and Examiner's responses regarding claims 4, 8 and 12 are as follows:

I) Appellants' argument: Regarding claim 4, "access checking logic disposed in said first view and programmed to omit said linkage," the Examiner merely stated "no access." In this regard, Appellant is entirely unclear how Bazinet teaches the specifically claimed limitations. A user having "no access" does not necessarily require that the linkage is omitted. Moreover, the Examiner has failed to establish that the access checking logic is disposed in the first view. Without the Examiner more clearly explaining the Examiner's analysis, Appellant cannot agree with the Examiner's assertion that Bazinet teaches these limitations (Brief, pages 7-8).

Examiner's response: Bazinet teaches of not providing (equivalent to applicant's omitting a linkage) access (equivalent to applicant's linkage) when the processing of checking authentication (equivalent to applicant's access checking logic) is indicated on the page (502 in figure 5, equivalent to applicant's first view, see, e.g., page 4, paragraph [0039]-[0040]) to the client's web browser. Therefore the processing of checking authentication (equivalent to applicant's access checking logic) is programmed to omit the linkage not allowed based on the authentication process.

Bazinet teaches that the portal application generates a page (equivalent to applicant's first view) to the client containing links (equivalent to applicant's linkage) corresponding to the backend applications that the authenticated user can access, based on the access privileges of the authenticated user (see, e.g., page 3, paragraph [0038] and step 416 in figure 4).

Therefore Bazinet clearly teaches of omitting backend application links for the unauthenticated user.

II) Appellants' argument: Regarding claim 4, the Examiner's analysis fails to consider the actual language of the claims. As claimed, the access logic is within the first view. The Examiner's assertion that the access checking logic is disposed in the portal application that provides the first view to the client fails to teach this limitation. Thus, the Examiner has failed to establish that Bazinet teaches the limitations for which the Examiner is relying upon Bazinet to teach (Brief, pages 7-8).

Examiner's response: Bazinet teaches of the access checking logic (processing of checking authentication, 406-414 in figure 4) processed in the portal application (102 in figure 4) and, the portal application provides the first view to the client (the portal application generate a page (equivalent to applicant's first view) to the client, see, e.g., page 3, paragraph [0038] and step 416 in figure 4). The portal application runs the access checking logic and shows the result of the access checking logic on the page to the client, wherein the page is equivalent to applicant's first view. Therefore, the access checking logic is disposed in the page by showing the results of the access checking logic process on the page.

The access checking logic is interpreted as a process checking which users are authenticated to access backend applications.

Claims are to be given their broadest reasonable interpretation during prosecution, and the scope of a claim cannot be narrowed by reading disclosed limitations into the claim. See In re Morris, 127 F.3d 1048, 1054, 44 USPQ2D 1023, 1027 (Fed. Cir. 1997); In re Zletz, 893 F.2d 319, 321, 13 USPQ2D 1320, 1322 (Fed. Cir. 1989); In re Prater, 415 F.2d 1393, 1404, 162 USPQ 541,550 (CCPA 1969). In addition, the law of anticipation does not require that a reference "teach" what an appellant's disclosure teaches. Assuming that reference is properly "prior art,'" it is only necessary that the claims "read on" something disclosed in the reference, i.e., all limitations of the claim are found in the reference, or "fully met" by it. Kalman v. Kimberly-Clark Corp., 713 F.2d 760, 772, 218 USPQ 781,789 (Fed. Cir. 1983).

III) Appellants' argument: Regarding claim 4, the Examiner's analysis, however, has failed to respond to Appellants' arguments. As previously argued, Bazinet already teaches authentication, and the Examiner has failed to establish any additional benefit arising from the Examiner's proposed modification. As such, one having ordinary skill in the art, while employing common sense, would not modify a reference when such a modification produces no identifiable benefit. Therefore, for the reasons presented above, Appellants respectfully submit that the Examiner has failed to establish that claim 1 is obvious in view of the combination of Bazinet and Vasandani (Brief, pages 8-9).

Examiner's response: Bazinet teaches the access control by authentication information (the authentication information includes user name and password combination, data on a smartcard etc, see, e.g., page 3, paragraph [0037]). Vasandani teaches the deficiency of role based access control (a userID-role database and a resource-role database for use in a web server to grant access to web resources to users, see, e.g., col. 2, lines 58-62), though it is obvious to include the user roles in the authentication information.

In this case, the obviousness can be established by modifying the authentication information taught of Bazinet to produce the claimed invention in the knowledge generally available to one or ordinary skill in the art.

By such modification, it provides various access levels based on the user role and provides efficient access control for each different role as well known to one or ordinary skill in the art.

IV) Appellants' argument: Regarding claims 8 and 12, the Examiner's analysis fails to consider the actual language of the claim. Allegedly generating a page based upon a checking authentication process is not the same as "processing said selected view to identify a method call to access checking logic," as claimed. In Bazinet, the alleged accessing checking logic (i.e., the checking authentication process) occurs prior to the alleged first view (i.e., the page) is generated. As such, there is no need for the first view to include a method call to access checking logic. On this basis alone, Bazinet fails to teach the limitations for which the Examiner is relying upon Bazinet to teach (Brief, pages 9-10).

Examiner's response: Bazinet teaches that the portal application runs the access checking logic and shows the result of the access checking logic on the page to the client, wherein the page is equivalent to applicant's first view. Therefore, the first view (the page to the client) identifies a method call to access checking logic by showing the result of the checking authentication process on the page.

B. Appellants' arguments and Examiner's responses regarding dependent claim 5 are as follows:

Appellants' argument: Regarding claim 5, claim 5 depends from independent claim 4, and Appellant incorporates herein the arguments previously advanced in traversing the imposed rejection of claim 1 under 35 U.S.C. §103 for obviousness based upon Bazinet and Vasandani. The tertiary reference to Schenk does not cure the argued deficiencies of the combination of Bazinet and Vasandani (Brief, page 11).

Examiner's response: The Appellant has not provided any substantive argument for claim 5 other than reiterating the same argument for claim 4. For the sake of brevity, the Board is respectfully referred to the points above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/J. S. P./

Examiner, Art Unit 2454

October 14, 2008

Conferees:

/Joseph E. Avellino/

Primary Examiner, Art Unit 2446

/Nathan J. Flynn/

Supervisory Patent Examiner, Art Unit 2454